LASEC

SECURITY AND CRYPTOGRAPHY LABORATORY

Family Name: .....

First Name: .....

Section: .....

Security and Cryptography

Midterm Exam (Solutions)

November 12th, 2009

Duration: 1 hour 45 min

This document consists of 8 pages.

Instructions

No documents are allowed apart from linguistic dictionaries.

Documents are *not* allowed apart from linguistic dictionaries.

Electronic devices are *not* allowed, except *simple calculators*.

Answers must be written on the exercises sheet.

This exam contains 3 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered.

Potential errors in these sheets are part of the exam.

You have to put your full name on the first page and have all pages *stapled*.

1 Modulo 101 Computation

Through *all* this exercise, we will let $p = 101$.

1. Show that p is a prime number.

   p is not divisible by any prime less than $\sqrt{p}$: 2, 3, 5, 7.

   What is the order of $\mathbf{Z}_p^*$?

   Since p is prime, $\#\mathbf{Z}_p^* = \varphi(p) = p - 1$.

2. If $x = \sum_{i=0}^{2\ell-1} d_i 10^i$ with $0 \leq d_i < 10$ for all i, show that

$$x \equiv \sum_{i=0}^{\ell-1} (-1)^i (d_{2i} + 10 d_{2i+1}) \pmod{101}$$

   Deduce an algorithm to compute x mod 101 easily.

   We have $x = \sum_{i=0}^{\ell-1} (d_{2i} + 10 d_{2i+1}) 100^i$ Since $100 \equiv -1 \pmod{101}$ we obtain the result. To reduce modulo 101, we simply take the decimal expansion, group digits by pair and apply the above formula iteratively until the result is less than 100 in absolute value. Then, if negative we add 101 and we are done.

3. Show that every element of $\mathbf{Z}_p^*$ has a unique 7th root and give an explicit formula to compute it (recall that $p = 101$).
   Application: Find the 7th root of 2 in $\mathbf{Z}_p^*$.

   7 is invertible modulo $p - 1$. Its inverse is 43 since $7 \times 43 = 301$ which is 1 modulo 100. So, the unique 7th root of x is x^{43} mod p.
   We compute 2^{43} mod 101 using the square and multiply algorithm. We have

$$\begin{aligned} 2^{43} &\equiv 2^{1+2\cdot(1+2^2\cdot(1+2^2))} \\ &\equiv 2 \times 4^{1+2^2\cdot(1+2^2)} \\ &\equiv 2 \times 4 \times 54^{1+2^2} \\ &\equiv 2 \times 4 \times 54 \times (-13)^2 \\ &\equiv 2 \times 4 \times 54 \times 68 \\ &\equiv 86 \end{aligned}$$

   We can check that $86^7 \equiv 2$.

4. Given $g \in \mathbf{Z}_p^*$ we let $y = g^{10} \bmod p$. Using 3 multiplications modulo p and 2 tests, give an algorithm with input y to decide whether g is a generator or not (recall that $p = 101$).
   Application: show that 2 is a generator.

Since $p-1 = 2^2 \times 5^2$, g is a generator iff $g^{\frac{p-1}{2}} \bmod p \neq 1$ and $g^{\frac{p-1}{5}} \bmod p \neq 1$. We have $g^{\frac{p-1}{2}} \equiv y^5$ and $g^{\frac{p-1}{5}} \equiv y^2$. So, we compute $a \equiv y^2$, $b \equiv a^2$, $c \equiv yb$ and we check that $a \not\equiv 1$ and $c \not\equiv 1$.
For $g = 2$, we compute

$$\begin{aligned} 2^{10} &\equiv 2^{2\cdot(1+2^2)} \\ &\equiv 4^{1+2^2} \\ &\equiv 4 \times 4^{2^2} \\ &\equiv 4 \times 16^2 \\ &\equiv 4 \times 54 \\ &\equiv 14 \end{aligned}$$

so $y = 14$. We now compute $a = 95$, $b = 36$, and $c = 100$. Since neither a nor c is 1, 2 is a generator.

5. Under which condition is x a quadratic residue in $\mathbf{Z}_p^*$?

It is equivalent to $x^{\frac{p-1}{2}} \bmod p = 1$.

6. Show that 5 is a quadratic residue in $\mathbf{Z}_p^*$.

We have

$$\begin{aligned} 5^{50} &\equiv 5^{2\cdot(1+2^3\times(1+2))} \\ &\equiv 25^{1+2^3\times(1+2)} \\ &\equiv 25 \times 25^{2^3\times(1+2)} \\ &\equiv 25 \times 19^{2^2\times(1+2)} \\ &\equiv 25 \times 58^{2\times(1+2)} \\ &\equiv 25 \times 31^{1+2} \\ &\equiv 25 \times 31 \times 31^2 \\ &\equiv 25 \times 31 \times 52 \\ &\equiv 1 \end{aligned}$$

so 5 is a quadratic residue.

7. Show that 10 is a 4th root of 1 in $\mathbf{Z}_p^*$.

We have $10^2 = 100 \equiv -1$ so $10^4 \equiv 1$.

8. Show that for all $y \in \mathbf{Z}_p^*$ we have that $y^{\frac{p-1}{4}}$ is 10^k for some $k \in \{0, 1, 2, 3\}$.

Since $\mathbf{Z}_p$ is a field, there are no more than 4 4th roots of 1 and these are all powers of 10: 1, 10, 100, and 91. Since $\left(y^{\frac{p-1}{4}}\right)^4 \equiv y^{p-1} \equiv 1$ in $\mathbf{Z}_p^*$, then $y^{\frac{p-1}{4}}$ must be one of these 4th roots of 1.

9. Show that $y^{\frac{p+3}{4}}$ can be written $y \times 10^k$.

We have $y^{\frac{p+3}{4}} = y \times y^{\frac{p-1}{4}} = y \times 10^k$.

10. Deduce that if x is a quadratic residue then either $x^{\frac{p+3}{8}}$ or $10x^{\frac{p+3}{8}}$ is a square root of x. Provide an algorithm to extract square roots in $\mathbf{Z}_p^*$.

If $x \equiv y^2$ then $x^{\frac{p+3}{8}} \equiv y^{\frac{p+3}{4}} \equiv y \times 10^k$ so its square is $x \times (-1)^k$. If k is even then this is a square root of x. If not, we multiply it by 10 and the power of 10 becomes even.
To compute square roots of quadratic residues, we just raise to the power $\frac{p+3}{8} = 13$ and we multiply by if it is not a square root.

11. Find a square root of 5.

We have

$$\begin{aligned} 5^{13} &\equiv 5^{1+2^2\times(1+2)} \\ &\equiv 5 \times 5^{2^2\times(1+2)} \\ &\equiv 5 \times 25^{2\times(1+2)} \\ &\equiv 5 \times 19^{1+2} \\ &\equiv 5 \times 19 \times 19^2 \\ &\equiv 5 \times 19 \times 58 \\ &\equiv 56 \end{aligned}$$

which is a square root of 5.

2 Guess my Age

I am human. My age is a prime number. Last year, it was multiple of 5. Next year, it will be multiple of 7. How old am I?
Provide a detailed proof of the result.

5 and 7 are coprime. The age is 1 modulo 5 and -1 modulo 7 Applying the Chinese remainder theorem, the age is $7 \times (7^{-1} \bmod 5) - 5 \times (5^{-1} \bmod 7)$ modulo 35. Since $7^{-1} \bmod 5 = 3$ and $5^{-1} \bmod 7 = 3$ this is 6 modulo 35. Since the age is positive, it can only be $6 + 35i$ for $i \geq 0$ integer. To be prime, it must be odd to i must be odd as well. The age is thus $41 + 70j$ for $j \geq 0$. Since 111 is not prime and 181 is too old to be human, the age can only be 41.

3 Authentication, Encryption and the OFB Mode of Operation

In many situations, an encryption scheme does provide confidentiality without authentication. In this exercise, we will look at some constructions and see whether they satisfy the above properties.

1. Recall what are the notions of confidentiality and authenticity.

> Let m be a message exchanged between two parties through a communication channel:
>
> - Confidentiality: adversary cannot get any information on m.
> - Authenticity: adversary cannot modify m.

2. Recall the definition of the Vernam cipher (also known as the one-time pad).

> Let K be a secret key and P the plaintext:
>
> - Encryption: $C = K \oplus P$
> - Decryption: $P = K \oplus C$

3. Although the Vernam cipher is perfectly secure, there are functions f such that the encryption C of P can be transformed to another ciphertext $C' \neq C$ that correctly decrypts to a message $P' = f(P)$ even when P is not known.
Show an example for f and this type of attack. Deduce that the Vernam cipher does not provide authentication.

> Given the funtion $f(P) = \bar{P}$, $C' = f(C) = \bar{C}$ will decrypt to $\bar{P}$.
> In general, flipping any bit of C will have the same effect on the corresponding plaintext.

Now, we consider the OFB mode of operation for a block cipher depicted in Fig. 1. The encryption under the key K is denoted E_K. Let $P = P_1 \| \dots \| P_n$ denote the plaintext and let $C = C_1 \| \dots \| C_n$ denote the ciphertext.

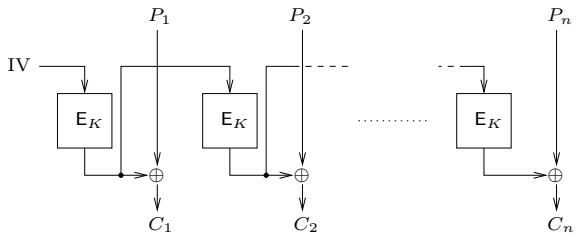

Figure 1: OFB mode

4. Give the name of two block ciphers. What is their block and key sizes?

DES: 64 bits, 56 bits.
AES: 128 bits, 128 bits.

5. Draw a picture for the decryption in OFB mode.

See Fig. 2

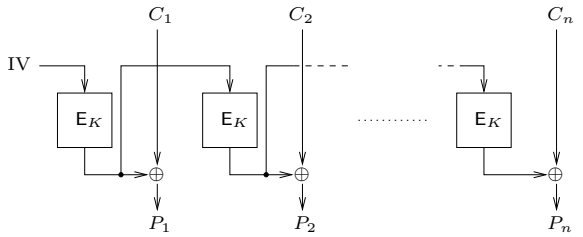

Figure 2: Decryption in OFB mode

6. Does the message manipulation attack on the Vernam cipher above still apply? Explain your answer.

Yes. This applies against any stream cipher.

7. Show how to perform a known plaintext attack in order to decrypt transmitted messages when the IV is secret but fixed.

See that:

$$C_i = P_i \oplus \mathsf{E}_K^{(i)}(\mathsf{IV})$$

for a known pair $(P = P_1 \| \ldots \| P_n, C = C_1 \| \ldots \| C_n)$.
The attack consists of computing $E_K(\mathsf{IV}), \ldots, E_K^{(n)}(\mathsf{IV})$ and using it to decrypt any message smaller than P (these do not depend on the message).

Any attempt to look at
the content of these pages
before the signal
will be severly punished.

Please be patient.